presumes a second cause which caused the first cause; and

requests said plurality of agent computers to collect logs to prove said presumed second cause; and

wherein each of said plurality of agent computers:

collects a log to prove said presumed first cause in response to a request from said manager computer;

sends said collected log to said manager computer; and

collects a log to prove said presumed second cause in response to a request from said manager computer.

9. The computer monitoring system according to claim 8,

wherein said manager computer displays an area of said computer system on the display, said area indicating a portion where the abnormal state is present, when presuming said first and second cause.

10. A computer monitoring system comprising:

a manager computer; and

(n+1) agent computers coupled to said manager computer over a network,

wherein said manager computer:

divides a collected log into n pieces of log information;

generates appendage information which recovers said log based on pieces of log information less than n;

distributes said n pieces of information and said appendage information to said (n+1) agent computers, respectively; and

wherein each of said (n+1) agent computers encrypts and memorizes respective one of said distributed log information and said appendage information.

11. A computer monitoring system comprising:

a manager computer; and

a plurality of computers coupled to said manager computer over a network,

wherein said manager computer monitors logs collected from said plurality of computers to be managed and detects suspicious behavior by comparing said logs or checking inconsistency of said logs.

12. The computer monitoring system according to claim 11,

wherein said suspicious behavior comprises at least one of a person other than regular users utilizing a computer to be managed illegally, and a person impersonating another person, and a person operating a computer to be managed beyond his/her permitted limit of operation.

13. The computer monitoring system according to claim 11, wherein each of said computers to be managed:

stores logs;

reports to said manager computer an alarm or a log more significant than a management level; and

changes said management level in response to an instruction from said manager computer; and

wherein said manager computer sets said management level in each of said computers to be managed.

14. The computer monitoring system according to claim 13, wherein each of said computers to be managed reports to said manager computer an alarm or a log requested by said manager computer; and

wherein said manager computer:

presumes causes resulting in contents from the contents of the reported alarm or log; and

collects a more detailed log to prove the presumption; and narrows down said presumed causes.

15. The computer monitoring system according to claim 11, wherein said manager computer:

displays icons of said computers to be managed on the monitor screen of said manager computer; and

changes an alarm sound or a color on said monitor screen according to a degree of suspicion for said computers to be managed performing suspicious behavior or a range of a display section showing possibility of existence of said computers to be managed performing suspicious behavior.

16. The computer monitoring system according to claim 11, wherein each of said computers to be managed:

adds a digital signature before storing or transferring a log;

adds redundant data to the log; and

recovers data of said log by using said redundant data when a part of said log is lost or altered.